UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA

BRYAN CURRY, TERRAN BROOKS, JERMAINE WILLIS, and BRIAN HOPPER on behalf of themselves and all others similarly situated,	)	Civil Action No.:
Plaintiff,	)	
v.	)	**CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**
SCHLETTER INC., Defendant.	)	

Plaintiffs, Bryan Curry, Terran Brooks, Jermaine Willis and Brian Hopper, individually and on behalf of all others similarly situated, by and through counsel, bring this action against the Schletter, (hereafter referred to collectively as "Schletter" or "Schletter") and allege as follows based upon personal knowledge, investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. On or about April 19, 2016, Schletter informed current and former employees that their 2015 W-2 tax form information had been given to an unauthorized third party by a Schletter employee. Falling for a well-known "phishing" or scam email scheme which human resources and accounting professionals have been warned about, the Schletter employee had complied with an email request to send unknown cyber criminals an unencrypted data file which contained either copies of W-2 statements or all of the sensitive personally identifying information ("PII") needed to fill out a W-2, including names, mailing addresses, Social Security numbers, and wage and withholding information (the "Data Disclosure"). The compromised data contained PII for every

W-2 employee[1], as categorized by the Internal Revenue Service ("IRS"), who worked at and received wages from Schletter during the time period of January 1, 2015 through December 31, 2015.

2. Almost immediately, the cyber criminals exploited Schletter's wrongful actions and began using the PII to commit actual fraud. Using the Social Security numbers disclosed by Schletter, the cyber criminals filed fraudulent tax returns in the names of employees and requested IRS account transcripts for other employees. These tax account transcripts provide data from most line items on a tax form, including adjusted gross income and tax withholdings, and indicate whether current year tax returns have been filed. But most importantly to cyber criminals, these IRS transcripts will also disclose Social Security numbers and wage information of both spouses for those filing joint tax returns. Thus, using the unlawfully obtained Social Security number of one employee, cyber criminals can request a tax transcript from the IRS to fraudulently obtain the Social Security of the employee's spouse.

3. The cyber criminals also used the PII to open fraudulent bank and financial accounts in the names of employees and to make financial transaction accounts.

4. As a consequence of the Data Disclosure, Class Members have suffered damages by taking measures to both deter and detect identity theft. Class Members have been required to take the time, which they otherwise would have dedicated to other life demands such as work, and effort to mitigate the actual and potential impact of the Data Disclosure on their lives including,

[1] In simplest terms, the IRS has two categories for workers: employees and independent contractors. For employees, payroll taxes are automatically deducted from paychecks and paid to the government through the employer. The employer reports the wages to the IRS at the end of the year on a W-2 form. Independent contractors are responsible for calculating and submitting their own payroll taxes. Companies report the wages paid to independent contractors on a Form 1099. *See*, *IRS Publication 15-A*, *available at* https://www.irs.gov/publications/p15a/ar02.html (last visited December 31, 2016).

inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's slippage, as is the case here.

5. No one can know what else the cyber criminals will do with the employees' PII. However, what is known is that the Schletter employees are now, and for the rest of their lives will be, at a heightened risk of further identity theft and fraud.

6. Even employees who registered for the identity theft service provided by Schletter have continued experiencing incidents of identity theft without any notice or alert from the service.

7. For all Class Members, fear and anxiety of identity theft or fraud is the new norm.

8. Plaintiffs bring this class action against Schletter for failing to adequately secure and safeguard the PII of Plaintiffs and the Class, failing to comply with industry standards regarding electronic transmission of PII, and for failing to provide timely and adequate notice to Plaintiffs and other Class members that their information had been stolen and precisely what types of information were stolen.

PARTIES

Plaintiff Bryan Curry

9. Plaintiff Bryan Curry is a citizen and resident of Cleveland County, North Carolina.

10. Mr. Curry is a former employee at Schletter, leaving his employment in or around September 2015.

11. Prior to the Data Disclosure, Plaintiff Bryan Curry had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

12. On or about April 2016, Plaintiff Bryan Curry and his wife received a letter from the IRS indicating that a request had been made to the IRS for a transcript of their tax account. The letter stated that the request had been made on April 17, 2016. Concerned that neither he nor his wife had made the request for this transcript, which included their Social Security Numbers, 2015 Adjusted Gross Income, 2015 Taxable Income, and tax withholding amounts, Mr. Curry contacted the IRS. He was instructed on the steps to take to report the identity theft and fraud.

13. Within days of receiving this letter from the IRS, Mr. Curry received a letter from Schletter advising that his personal information had been released by his former employer to an unauthorized third party.

14. As a result of the Data Disclosure, Mr. Curry has spent, and will continue to spend, numerous hours monitoring his credit reports and completing the IRS paperwork necessary to protect himself from future incidents of identity theft or fraud.

15. Most importantly, Mr. Curry has been the victim of identity theft as a result of the Data Breach and will continue to be at heightened risk for further tax fraud and identity theft and their attendant dangers for years to come.

Plaintiff Terran Brooks

16. Plaintiff Terran Brooks is a citizen and resident of Cleveland County, North Carolina.

17. Mr. Brooks is a current employee at Schletter whose PII was disclosed without his authorization to an unknown third party as a result of the Data Disclosure.

18. Prior to the Data Disclosure, Plaintiff Terran Brooks had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

19. On or about June 16, 2016, Plaintiff Terran Brooks received a letter from Discover Bank, with which Mr. Brooks has never had an account. The letter stated that Discover Bank was returning a check in the amount of $5,000 that it had received for a deposit. The reason for the return was stated to be "account closed." The check was dated June 13, 2016, was shown to be sent from Mr. Brooks, with his correct address listed, and paid to the order of Discover Bank. No issuing bank was listed, but the check contains instructions for questions to be directed to "Online Bill Payment Processing Center."

20. Upon information and belief, Online Bill Payment Processing Center is a service that some banks use to provide online bill paying services for their customers. The internet contains reports from consumers who have received and attempted to deposit such checks stating that monies initially credited to their accounts by using these checks were withdrawn by others.

21. As Mr. Brooks has never had an account with Discover Bank, he called the customer service number on the letter and was directed to the bank's Fraud Unit. He then followed up with a call directly to Discover Bank's Fraud Unit to report the fraud that had occurred in his name.

22. Because his personal information was disclosed as a result of the Data Disclosure, Mr. Brooks was automatically enrolled in the Core-ID Identity Theft Protection service by Schletter. His enrollment, along with all others affected by the Data Disclosure, became effective April 13, 2016.

23. Since being enrolled in the CoreID service, Mr. Brooks has received no notice or alert from the service advising of any potential fraudulent activity—not even when the fraudulent

activity with Discover Bank occurred.

24. As a result of the Data Disclosure, Plaintiff Terran Brooks has spent time and effort addressing this fraud.

25. Most importantly, Mr. Brooks has been the victim of identity theft as a result of the Data Breach and will continue to be at heightened risk for further tax fraud and identity theft and their attendant dangers for years to come.

Plaintiff Jermaine Willis

26. Plaintiff Jermaine Willis is a citizen and resident of Cleveland County, North Carolina.

27. Mr. Willis is a current employee at the Schletter facility located in Shelby, North Carolina whose PII was disclosed without his authorization to an unknown third party as a result of the Data Disclosure.

28. To his knowledge, prior to the Data Disclosure, Mr. Willis had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

29. In or around the middle of May 2016, Plaintiff Jermaine Willis received a letter, dated May 13, 2016, from the Internal Revenue Service ("IRS") advising that it appeared someone using his personal information had filed a 2015 tax return and the IRS had reason to suspect that the return was fraudulent. Since Mr. Willis had not yet filed his 2015 tax return, he realized from this letter that he had been the victim of identity theft. Mr. Willis was instructed by the IRS on the extra steps that will be needed for the next few years to file a paper return with verification of his identity.

30. On or about July 28, 2016, Mr. Willis received an "Overdraft Coverage

Confirmation (Acceptance)" from SunTrust Bank regarding an account in his name. As Mr. Willis did not maintain any financial accounts with SunTrust, he realized that the account must have been fraudulently opened in his name.

31. Subsequently, Mr. Willis received a letter from SunTrust bank dated July 28, 2016, advising that SunTrust Fraud Risk Management had closed an account in his name after a review of the account. This communication convinced Mr. Willis that he, once again, had been the victim of identity theft.

32. As a result of these communications, Mr. Willis spent time contacting SunTrust to report that the referenced account had been opened without his authorization and to make certain that any fraudulent accounts were closed summarily. SunTrust confirmed that they had taken such action to close the referenced account.

33. Because his personal information was disclosed as a result of the Data Disclosure, Mr. Willis was automatically enrolled in the Core-ID Identity Theft Protection service by Schletter. His enrollment, along with all others affected by the Data Disclosure, became effective April 13, 2016.

34. Since being enrolled in the CoreID service, Mr. Willis has received no notice or alert from the service advising of any potential fraudulent activity—not even when the fraudulent account was opened at SunTrust Bank.

35. Plaintiff Jermaine Willis has spent and will continue to spend a significant amount of time, effort and expense countering the repercussions of the tax fraud and identity theft.

36. Most importantly, Mr. Willis has been the victim of identity theft as a result of the Data Breach and will continue to be at heightened risk for further tax fraud and identity theft and their attendant dangers for years to come.

Plaintiff Brian Hopper

37. Plaintiff Brian Hopper is a citizen and resident of Cleveland County, North Carolina.

38. Mr. Hopper is a former employee at the Schletter facility located in Shelby, North Carolina whose PII was disclosed without his authorization to an unknown third party as a result of the Data Disclosure.

39. To his knowledge, prior to the Data Disclosure, Mr. Hopper had no knowledge of ever being the victim of identity theft or being involved in a data breach incident.

40. As a result of the Data Disclosure, Plaintiff Brian Hopper has been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring him to spend time and effort to mitigate the actual and potential impact of the Data Disclosure by, inter alia, closely monitoring his credit reports and financial accounts.

Defendant Schletter, Inc.

41. Defendant Schletter, Inc. ("Schletter" or "Defendant") is a Delaware corporation with its principal place of business in Shelby, North Carolina.

42. Schletter has manufacturing facilities in North Carolina and Arizona, and sales representatives in California, Connecticut and Tennessee.

JURISDICTION AND VENUE

43. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because there are more than 100 Class Members, the class contains members of

diverse citizenship from Defendant, and the amount in controversy exceeds $5,000,000 exclusive of costs and interests.

44. This Court has personal jurisdiction over Schletter because its U.S. headquarters is in this District and Schletter is authorized to and does conduct substantial business in North Carolina, and in this District.

45. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Schletter's U.S. headquarters is in this District, Schletter regularly conducts business in this District, and a substantial part of the events or omissions giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

46. As a condition of employment, Schletter requires that employees entrust it with certain personal information. In its ordinary course of business, Schletter maintains personal and tax information, including name, address, zip code, date of birth, wage and withholding information, and Social Security number, of its current and former employees. Plaintiffs and members of the proposed Class, as current and former employers, relied on Schletter to keep this information confidential and securely maintained.

47. On or about April 19, 2016, Schletter mailed a form letter[2] to current and former employees, advising that 2015 W-2 tax form information had been "sent to an unauthorized third party in response to the W-2 phishing email scam." In this letter, Schletter recognized the "value" and "privacy" of this personal information.

[2] A copy of the April 19, 2016 letter is attached hereto as Exhibit A.

48. The letter indicated that Schletter had learned of the "data security incident" on or about April 13, 2016, but no information was given as to the actual date when the tax data had been disclosed by Schletter.

49. The April 19, 2016 letter from Schletter was accompanied by an additional document entitled "Steps You Can Take to Further Protect Your Information." [3] Buried within this document was a statement that, at some later date in the future, Schletter would be offering credit monitoring and identity theft protection services to those affected for a one year period. This obscured statement indicated that individuals would have only 30 days to enroll once the enrollment instructions were ultimately provided.

50. Schletter sent former and current employees a "Core ID Identity Theft Protection Welcome Letter" on or about April 25, 2016.[4] The form letter stated that "after careful consideration," Schletter had decided to extend the identity theft protection and credit monitoring coverage to 24 months, from the initial offer of only 12 months. The letter advised that current and former employees were "already currently enrolled" in the service.

51. This April 25, 2016 letter was accompanied by a "Welcome Letter" from Core ID,[5] the provider of the identity theft protection and credit monitoring coverage. This letter advised recipients that they were "enrolled and protected with ARX-ID Complete" coverage with a retroactive effective date of April 13, 2016, the date Schletter *discovered* that it had disclosed its employees' personal information. Once again, no information was provided as to the actual date of the Data Disclosure by Schletter.

[3] A copy of this document is attached hereto as Exhibit B.
[4] A copy of the April 25, 2016 letter is attached hereto as Exhibit C.
[5] A copy of the CoreID Welcome Letter is attached hereto as Exhibit D.

52. This Data Disclosure was caused by Schletter's voluntary disclosure of the PII of its current and former employees, ironically at a time in the calendar year when W-2 information is most vital and valuable.

53. Schletter was not without warning of this phishing email scam, yet it failed to implement adequate measures to protect its employees' PII. Schletter's negligence in safeguarding its employees' PII is exacerbated by the repeated warnings and alerts, not only of the increasing risk of general email scams, but of the actual W-2 phishing email scam it chose to ignore and, thus, fell prey to.

54. On August 27, 2015, the Federal Bureau of Investigation ("FBI") issued a report warning of the increasingly common scam, known as Business Email Compromise, in which companies fall victim to phishing emails.[6] Most importantly, this report called attention to the significant spike in scams, also referred to as spoofing, in which cyber criminals send emails that appear to have initiated from the CEO or other top level executive at the target company.

55. Business Email Compromise or spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. For example, spoofed email may purport to be from someone in a position of authority within a company asking for sensitive data such as passwords or employee information that can be used for a variety of criminal purposes. A tell-tale sign of a spoofing e-mail is an "urgent" request from a company "executive" requesting that confidential information be provided via email.

56. As noted by cybersecurity journalist Brian Krebs, this type of fraud "usually begins with the thieves either phishing an executive and gaining access to that individual's email account

---

[6] *See, Public Service Announcement, Business Email Compromise*, Alert No. I-082715a-PSA (August 27, 2015), *available at* https://www.ic3.gov/media/2015/150827-1.aspx (last visited December 30, 2016.).

or emailing employees from a look-alike domain that is one or two letters off from the company's true domain name." [7]

57. Spoofing fraud has been on a steady incline in recent years. The FBI recently issued an alert stating that from October 2013 through February 2016, law enforcement received reports from over 17,000 victims of "spoofing" scams which resulted in more than $2.3 billion in losses. Since January 2015, the FBI has seen a 270% increase in identified victims and exposed loss from spoofing scams.[8]

58. Companies can mount two primary defenses to spoofing scams: employee education and technical security barriers. Employee education is the process of adequately making employees aware of common spoofing scams and implementing company-wide policies requiring the request or transfer of sensitive personal or financial information only through secure sources to known recipients. Employee education and secure file-transfer protocols provide the easiest method to assist employees in properly identifying fraudulent e-mails and prevent unauthorized access of personal and tax information.

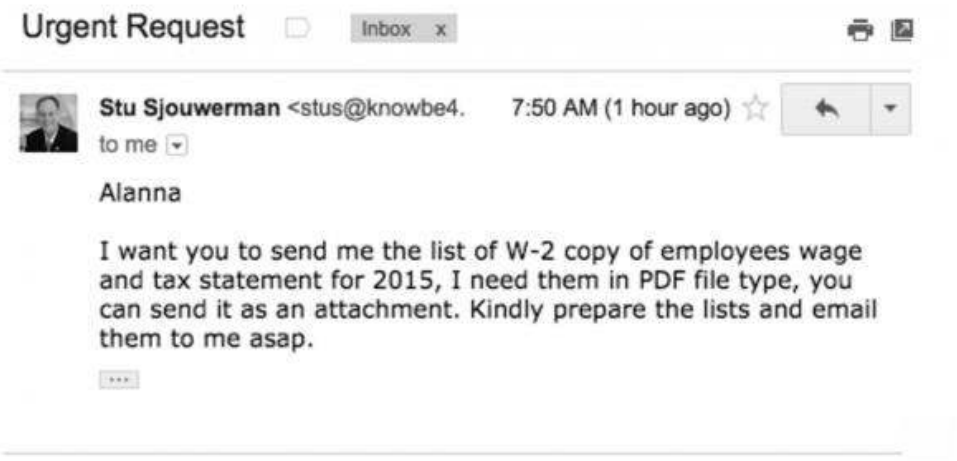
59. From a technical perspective, companies can also greatly reduce the flow of spoofing e-mails by implementing certain security measures governing e-mail transmissions. Companies can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it much harder for malicious senders to disguise their identities. Companies can also use email authentication that blocks email streams that have not been properly authenticated.

---

[7] Brian Krebs, *FBI: $2.3 Billion Lost to CEO Email Scams*, KREBS ON SECURITY (April 7, 2016), *available at* http://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/ (last visited December 31, 2016).

[8] *FBI Warns of Dramatic Increase in Business E-Mail Scams* (April 4, 2016), *available at* https://www.fbi.gov/phoenix/press-releases/2016/fbi-warns-of-dramatic-increase-in-business-email-scams (last visited December 31, 2016).

60. On February 24, 2016, cybersecurity journalist Brian Krebs warned of the precise scam which snared Schletter in a blog that said all it needed to say in its title: Phishers Spoof CEO, Request W2 Forms.[9] Krebs warned that cybercriminals were attempting to scam companies by sending false emails, purportedly from the company's chief executive officer, to individuals in the human resources or accounting department asking for copies of W-2 data for all employees. Krebs even provided an example of such an email that had been sent to another company:



61. Further, on March 1, 2016, the IRS issued an alert to payroll and human resources professionals warning of the same scheme. In precise detail, the alert stated:

> The Internal Revenue Service today issued an alert to payroll and human resources professionals to beware of an emerging phishing email scheme that purports to be from company executives and requests personal information on employees.
>
> The IRS has learned this scheme — part of the surge in phishing emails seen this year — already has claimed several victims as payroll and human resources offices mistakenly email payroll data including Forms W-2 that contain Social Security numbers and other personally identifiable information to cybercriminals posing as company executives.

[9] Brian Krebs, *Phishers Spoof CEO, Request W2 Forms*, KREBS ON SECURITY *available at* http://krebsonsecurity.com/2016/02/phishers-spoof-ceo-request-w2-forms/ (last visited December 30, 2016).

> "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments," said IRS Commissioner John Koskinen. "If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees." [10]

62. Despite the widespread prevalence of spoofing aimed at obtaining confidential information from employers and despite the warnings of the 2016 tax season W-2 email scam, Schletter provided its employees with unreasonably deficient training on cybersecurity and information transfer protocols prior to the Data Disclosure.

63. Schletter failed to adequately train its employees on even the most basic of cybersecurity protocols, including:

a. How to detect phishing and spoofing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoidance of responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information;

e. Implementing guidelines for maintaining and communicating sensitive data; and,

f. Protecting sensitive employee information, including personal and financial

[10] IRS, *IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s*, IR-2016-34 (March 1, 2016), *available at* https://www.irs.gov/uac/Newsroom/IRS-Alerts-Payroll-and-HR-Professionals-to-Phishing-Scheme-Involving-W2s (last visited December 30, 2016).

information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients.

64. Schletter's failures handed to criminals the PII of Plaintiffs and other Class Members and put Plaintiffs and the Class at serious, immediate and ongoing risk for identity theft and fraud. The practice with such breaches is that the cyber criminals will use the PII, as they have done here, to file false tax returns immediately. Access to W-2 information permits identity thieves to quickly and easily file fraudulent tax returns using the victim's information to obtain a fraudulent refund. The IRS will direct deposit the refund to the bank account or prepaid debit card (which are virtually untraceable) provided by the thief.

65. Additionally, the cyber criminals will continue to use the PII to open up fraudulent financial accounts, as they have done here, in exploitation of and injury to Plaintiffs and Class Members.

66. The Data Disclosure was caused by Schletter's violation of its obligation to abide by best practices and industry standards concerning the security of its computer and payroll processing systems. Schletter failed to comply with security standards and allowed its employees' PII to be compromised by failing to implement security measures that could have prevented or mitigated the Data Disclosure. Schletter failed to implement even the most basic of security measures to require encryption of any data file containing PII sent electronically, even within the company.

67. Schletter failed to ensure that all personnel in its human resources and accounting departments were made aware of this well-known and well-publicized phishing email scam.

68. Schletter failed to timely disclose the extent of the Data Disclosure, failed to

individually notify each of the affected individuals in a timely manner, and failed to take other reasonable steps to clearly and conspicuously inform Plaintiffs and the other Class Members of the nature and extent of the Data Disclosure. By failing to provide adequate and timely notice, Schletter prevented Plaintiffs and Class Members from protecting themselves from the consequences of the Data Disclosure.

69. The ramifications of Schletter's failure to keep its employees' PII secure are severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

71. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

72. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[13]

73. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, as they have done here, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

74. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

75. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

76. Based on the foregoing, the information compromised in the Data Disclosure is significantly more valuable than the loss of, say, credit card information in a large retailer data

[13]Social Security Administration, Identity Theft and Your Social Security Number, *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited December 30, 2016).

[14] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, *available at* http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited December 31, 2016).

breach such as those that occurred at Target and Home Depot. Victims affected by those retailer breaches could avoid much of the potential future harm by cancelling credit or debit cards and obtaining replacements. The information compromised in the Schletter Data Disclosure is difficult, if not impossible, to change—Social Security number, name, date of birth, employment information, income data, etc.

77. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[15]

78. Despite all of the publically available knowledge of the continued compromises of PII, and alerts regarding the actual W-2 phishing email scam perpetrated, Schletter's approach to maintaining the privacy of its employees PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

79. Schletter failed to provide compensation to Plaintiffs and Class Members victimized in this Data Disclosure. Schletter has not offered to provide any assistance or compensation for the costs and burdens – current and future - associated with the identity theft and fraud resulting from the Data Disclosure. Schletter has not offered employees any assistance in dealing with the IRS or state tax agencies. Schletter has not offered to reimburse employees for the costs – current and future – incurred as a result of falsely filed tax returns.

80. To date, Schletter has offered its employees only two years of identity theft

[15] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited December 29, 2016).

protection through Core ID's ARX-ID Complete service. Schletter has not offered to reimburse the cost of identity theft protection services purchased by employees before Schletter gave notice that it would pay for such services.

81. In any event, the offered ARX-ID service is inadequate to protect the Plaintiffs and Class Members from the threats they face, particularly in light of the PII stolen. Many websites that rank identity theft protection services are critical of ARX-ID. NextAdvisor does not even include Core ID in its rankings of identity theft protection services.[16] BestIDTheftCompanys.com ranks ARX-ID at number 11 on its list of companies with a mere score of 5.2 out of 10, noting that the service does not offer credit monitoring, reports or scores, as do most of their competition. Instead, Core ID sends subscribers annual reminders to request their free credit report.[17] The lack of this feature ensures that Schletter employees will continue to spend their own time each year to monitor their credit reports for fraudulent activity.

82. As noted above, Plaintiffs Brooks and Willis, and other Class Members, have experienced fraudulent activity since their automatic enrollment in the CoreID service but have not received even an alert from the service indicating the presence of suspicious activity. The enrollment in the CoreID service provided by Schletter has neither prevented Plaintiffs and Class Members from experiencing fraudulent activity using their PII nor alerted them that they had fallen victim to identity theft.

83. As a result of Schletter's failures to prevent the Data Disclosure, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety and emotional distress. They have suffered or are at increased risk of suffering:

[16] See, http://www.nextadvisor.com/identity_theft_protection_services/index.php (last visited November 13, 2016).
[17] *See*, https://bestidtheftcompanys.com/company/core-id/ (last visited November 13, 2016).

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise, publication and/or theft of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

f. Unauthorized use of compromised PII;

g. The continued risk to their PII, which remains in the possession of Schletter and is subject to further breaches so long as Schletter fail to undertake appropriate measures to protect the PII in their possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

CLASS ACTION ALLEGATIONS

84. Plaintiffs bring this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23. This action satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of the provisions of Rule 23.

85. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All current and former Schletter employees whose PII was compromised as a result of the Data Disclosure.

86. In the alternative to the Nationwide Class, and pursuant to Federal Rule of Civil Procedure 23(c)(5), Plaintiffs seek to represent the following state class only in the event that the Court declines to certify the Nationwide Class above. Specifically, the state class consists of the following:

> All current and former Schletter employees who currently reside in North Carolina and whose PII was compromised as a result of the Data Disclosure.

87. Excluded from the Class are the officers, directors and legal representatives of Schletter and the judges and court personnel in this case and any members of their immediate families.

88. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is estimated to be at or above 200. The exact number is generally ascertainable by appropriate discovery as Schletter had knowledge of the employees whose PII was in the data file it disclosed.

89. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Schletter had a duty to protect the PII of Class Members;

b. Whether Schletter failed to adequately safeguard the PII of Class Members;

c. Whether Schletter timely, adequately, and accurately informed Class Members that

their PII had been compromised;

d. Whether Schletter failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Disclosure;

e. Whether Schletter engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Class Members;

f. Whether Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Schletter' wrongful conduct;

i. Whether Plaintiffs and the members of the Class are entitled to restitution as a result of Schletter' wrongful conduct; and,

j. Whether Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Disclosure.

90. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other class member, was disclosed by Schletter. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct described above and were subject to Schletter's unfair and unlawful conduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all Class Members.

91. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class members. Plaintiffs have retained

counsel experienced in complex consumer class action litigation, and Plaintiffs intend to prosecute this action vigorously.

92. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large corporate Schletter. Further, even for those class members who could afford to litigate such a claim, it would still be economically impractical.

93. The nature of this action and the nature of laws available to Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and the Class for the wrongs alleged because Schletter would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each member of the Class to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

94. The litigation of the claims brought herein is manageable. Schletter' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

95. Adequate notice can be given to Class Members directly using information maintained in Schletter's records.

96. Unless a Class-wide injunction is issued, Schletter may continue in its failure to properly secure the PII of Class Members, Schletter may continue to refuse to provide proper notification to Class Members regarding the Data Disclosure, and Schletter may continue to act unlawfully as set forth in this Complaint.

97. Schletter have acted, or refused to act, on grounds that apply generally to the Class, making final injunctive and declaratory relief appropriate to the Class as a whole. Schletter' acts and omissions are the direct and proximate cause of damage described more fully elsewhere in this Complaint.

98. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, before the Court determines whether certification is appropriate and as the parties engage in discovery.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of the Class)

99. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

100. As a condition of their employment, employees were obligated to provide Schletter with certain PII, including their date of birth, mailing addresses and Social Security numbers.

101. Plaintiffs and the Class Members entrusted their PII to Schletter on the premise and

with the understanding that Schletter would safeguard their information.

102. Schletter had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed.

103. Schletter had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing Schletter's security systems to ensure that Plaintiffs and Class members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of employees' personal and tax information.

104. Plaintiffs and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Schletter knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, the current cyber scams being perpetrated on companies, and that it had inadequate employee training and education and IT security protocols in place to secure the PII of Plaintiffs and the Class.

105. Schletter's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Schletter's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Disclosure as set forth herein. Schletter's misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII of Plaintiffs and Class Members.

106. Plaintiffs and the Class Members had no ability to protect their PII that was in Schletter's possession.

107. Schletter was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Disclosure.

108. Schletter had and continues to have a duty to timely disclose that the PII of Plaintiffs and Class Members within its possession might have been compromised and precisely the types of information that were compromised and when. Such timely notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate and repair any identity theft and the fraudulent use of their PII by third parties.

109. Schletter had a duty to have proper procedures in place to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

110. Schletter has admitted that the PII of Plaintiffs and Class Members was wrongfully disclosed as a result of the Data Disclosure.

111. Schletter, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within Schletter's possession or control.

112. Schletter improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations and practices at the time of the Data Disclosure.

113. Schletter failed to heed industry warnings and alerts issued by the IRS to provide adequate safeguards to protect employees' PII in the face of increased risk of a current phishing email scheme being perpetrated.

114. Schletter, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and

prevent dissemination of its employees' PII.

115. Schletter, through its actions and/or omissions, unlawfully breached its duty to timely and adequately disclose to Plaintiff and Class Members the existence, timing and scope of the Data Disclosure.

116. But for Schletter's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

117. There is a close causal connection between Schletter's failure to implement security measures to protect the PII of current and former employees and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class.

118. As a result of Schletter's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with addressing false tax returns filed; current and future out-of-pocket costs in connection with preparing and filing tax returns; loss or delay of tax refunds as a result of fraudulently filed tax returns; out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Disclosure.

SECOND CAUSE OF ACTION
Invasion of Privacy
(On Behalf of the Class)

119. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

120. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendant owed a duty to its employees, including Plaintiffs and Class Members,

to keep their PII contained as a part thereof, confidential.

122. Defendant intentionally released to unknown and unauthorized third parties a file containing the PII of Plaintiffs and Class Members.

123. Defendant intentionally allowed unauthorized and unknown third parties unfettered access to and examination of the PII of Plaintiffs and Class Members.

124. The unauthorized release to, custody of and examination by unauthorized third parties of the PII of Plaintiffs and Class Members, especially where the information includes Social Security numbers and wage information, would be highly offensive to a reasonable person.

125. Defendant's intrusion upon the privacy of Plaintiffs and Class Members was offensive and objectionable.

126. The intrusion was into a place or thing which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII to Schletter as part of their employment, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their authorization.

127. As a proximate result of the above acts and omissions of Schletter, the PII of Plaintiffs and Class Members was disclosed to and used by third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

128. Unless and until enjoined, and restrained by order of this Court, Schletter' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Schletter can be viewed, distributed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Class)

129. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

130. Plaintiffs and Class members were required to provide their PII, including names, addresses, Social Security numbers, and other personal information, to Schletter as a condition of their employment.

131. Implicit in the employment agreement between the Schletter and its employees was the obligation that both parties would maintain information confidentially and securely.

132. Schletter had an implied duty of good faith to ensure that the PII of Plaintiffs and Class members in its possession was only used to provide agreed-upon compensation and other employment benefits from Schletter.

133. Schletter had an implied duty to reasonably safeguard and protect the PII of Plaintiffs and Class members from unauthorized disclosure or uses.

134. Additionally, Schletter implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

135. Plaintiffs and Class members fully performed their obligations under the implied contract with Schletter. Schletter did not.

136. Plaintiffs and Class members would not have provided their confidential PII to Schletter in the absence of their implied contracts with Schletter, and would have instead retained the opportunity to control their PII for uses other than compensation and employment benefits from Defendant.

137. Schletter breached the implied contracts with Plaintiffs and Class members by

failing to reasonably safeguard and protect Plaintiffs' and Class members' PII, which was compromised as a result of the Data Disclosure.

138. Schletter's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiffs and Class members to provide their PII as a condition of employment in exchange for compensation and benefits.

139. As a direct and proximate result of Schletter's breach of its implied contacts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their PII, which remain in Schletter's possession and is subject to further unauthorized disclosures so long as Schletter fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and, (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Disclosure for the remainder of the lives of Plaintiffs and Class members.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of the Class)

140. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

141. Schletter was a fiduciary, as an employer created by its undertaking, to act primarily for the benefit of its employees, including Plaintiffs and Class members, in matters connected with their employment.

142. Schletter had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their employer/employee relationship, in particular to keep income records and report such information in a form W-2 to the IRS.

143. Schletter breached its duty of care to Plaintiffs and Class members to ensure that their PII and W-2 data was not disclosed without authorization or used for improper purposes by failing to provide adequate protections to the information and by voluntarily disclosing the information, in an unencrypted format, to an unknown and unauthorized third party.

144. As a direct and proximate result of the Schletter's actions alleged above, the Plaintiffs and Class members have suffered actual damages.

FIFTH CAUSE OF ACTION
Violation of the North Carolina Identity Theft Protection Act
N.C. Gen. Stat. § 75-62 *et seq*.
(On Behalf of the Class)

145. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

146. Schletter is a "business" under N.C. Gen. Stat. § 75-6 1(1).

147. Schletter intentionally communicated or otherwise made available to unknown third parties the Social Security numbers of Plaintiffs and Class Members in violation of N.C. Gen.

Stat. § 75-62(a)(1).

148. Schletter intentionally disclosed the Social Security numbers of Plaintiffs and Class Members to unknown third parties without the consent and authorization of Plaintiffs and Class Members.

149. As set forth above, based upon the repeated and widespread warnings regarding the W-2 phishing scam, Schletter knew or in the exercise of reasonable diligence would have had reason to believe that the third party sending the request for the W-2 data lacked a legitimate purpose for obtaining the Social Security numbers of Plaintiffs and Class Members.

150. Pursuant to N.C. Gen. Stat. § 75-62(d), Schletter's violation of the North Carolina Identity Theft Protection Act is a violation of the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. § 75-1.1.

FOURTH CAUSE OF ACTION
Violation of the North Carolina Unfair and Deceptive Trade Practices Act
N.C. Gen. Stat. § 75-1.1., *et seq*.
(On Behalf of the Class)

151. Plaintiffs restate and realleges paragraphs 1 through 98 as if fully set forth herein.

152. It is appropriate to apply North Carolina law to the nationwide class claims because North Carolina's interest in this litigation exceeds that of any other state.

153. As discussed above, Schletter's U.S. headquarters are located in North Carolina. Upon information and belief, the acts leading to the disclosure of employees' PII occurred at a Schletter facility in North Carolina. Based upon the foregoing, the policies, practices, acts and omissions giving rise to this Action emanated from Schletter's headquarters and facilities in North Carolina.

154. Schletter were engaged in practices affecting commerce by the actions described above within the meaning of N.C. Gen. Stat. §75-1.1.

155. The conduct of Schletter alleged above constitutes an unfair and deceptive trade practice in violation of N.C. Gen. Stat. § 75-1.1(a) which provides:

> Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

156. Schletter' acts or practice of failing to employ reasonable and appropriate security measures to protect the PII of Plaintiffs and Class Members constitute unfair or deceptive acts or practices the North Carolina Unfair and Deceptive Trade Practices Act (UDTPA).

157. Schletter further violated UDTPA by violating North Carolina's Identity Theft Protection Act (ITPA), N.C. Gen. Stat. § 75-60, *et. seq*. (ITPA).

158. Defendant violated ITPA by:

a. Failing to prevent the personal information of employees from falling into unauthorized hands;

b. Failing to make reasonable efforts to safeguard and protect the personal information, particularly Social Security numbers, of employees; and

c. Failing to provide adequate notice of the security breach to affected employees upon discovery that their system had been compromised and personal information had been stolen.

159. Schletter violated UDTPA by intentionally communicating and disclosing its employees' Social Security numbers, without written consent, to a third party, which it had reason to believe lacked a legitimate purpose for obtaining the Social Security numbers, in direct violation of N.C.G.S. § 75-62.

160. Schletter willfully concealed, suppressed, omitted and failed to inform Plaintiffs

and Class Members of the material facts as described above.

161. Plaintiffs and Class Members have suffered ascertainable losses as a direct result of Schletter' unconscionable acts or practices, and unfair or deceptive acts or practices.

162. As a direct and proximate result of the injury caused by the unfair and deceptive trade practices of the Schletter, Plaintiffs and Class Members are entitled to relief, including actual and treble damages, under N.C.G.S. § 75-1.1 and 75-16. Further, the unlawful acts and omissions as set forth above were willful violations entitling Plaintiffs to attorneys' fees, under N.C.G.S. § 75-16.1. Further, similarly situated members of the proposed Class are likewise entitled to remedies due to the injury they have suffered as a result of the unfair and deceptive trade practices.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs on behalf of themselves and all others similarly situated, pray for relief as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;

B. A mandatory injunction directing Schletter to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Schletter provide notice to each member of the Class relating to the full nature and extent of the Data Disclosure and the disclosure of PII to unauthorized persons;

D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of attorneys' fees and costs;

F. For treble damages pursuant to N.C. Gen. Stat § 75-16 and for Plaintiffs' costs incurred; and,

G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: January 3, 2017

Respectfully submitted,

/s/ Jean Sutton Martin
JEAN SUTTON MARTIN
North Carolina Bar Number 25703
jean@jsmlawoffice.com
LAW OFFICE OF JEAN SUTTON MARTIN PLLC
2018 Eastwood Road Suite 225
Wilmington, NC 28403
Telephone: (910) 292-6676
Facsimile: (888) 316-3489
Email:

/s/ John A. Yanchunis
JOHN A. YANCHUNIS*
Florida Bar No. 324681
jyanchunis@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiffs and the Proposed Class

** Special Admission to be submitted*